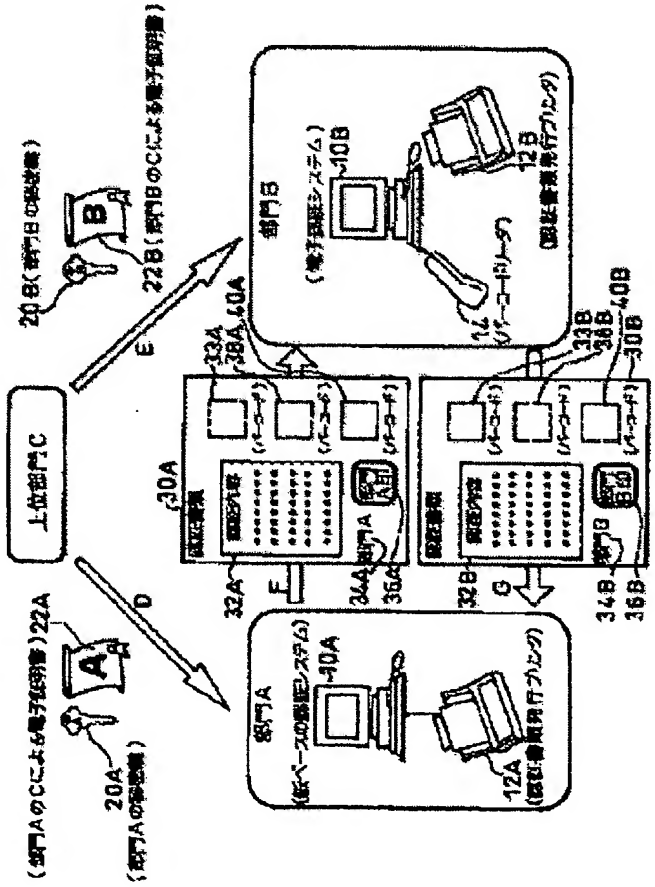
AUTHENTICATION DOCUMENT, AUTHENTICATION FORM, AND SYSTEM FOR ISSUING AND VERIFYING AUTHENTICATION DOCUMENT

Publication number: JP2002062803
Publication date: 2002-02-28
Inventor: MORITA YORIKO
Applicant: DAINIPPON PRINTING CO LTD
Classification:
- international: ***B42D11/00; G06F19/00; G06K19/06; G06Q10/00; G06Q50/00; G07D7/20; G09C1/00;*** **B42D11/00; G06F19/00; G06K19/06; G06Q10/00; G06Q50/00; G07D7/00; G09C1/00;** (IPC1-7): G09C1/00; B42D11/00; G06F17/60; G06F19/00; G06K19/06; G07D7/20
- European:
Application number: JP20000252054 20000823
Priority number(s): JP20000252054 20000823

Abstract of **JP2002062803**

PROBLEM TO BE SOLVED: To provide an authentication document applicable to both of an electronic authentication system and a paper-base authentication system.
SOLUTION: Visibly confirmable authentication contents 30A, 30B, authenticator information 34A, 34B, and authenticator's seal imprints 36A, 36B are described in authentication certificates 30A, 30B together with bar codes 33A, 33B of authentication contents data in which the authentication contents 32A, 32B are described, bar codes 38A, 38B of electronic signature data enciphering the authentication contents data, and bar codes 40A, 40B of electronic certificate data of the authenticator.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－62803
（P2002－62803A）
(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	３Ｅ０４１
				６４０Ｂ	５Ｂ０３５
Ｂ４２Ｄ	11/00		Ｂ４２Ｄ　11/00	Ｕ	５Ｊ１０４
Ｇ０６Ｆ	17/60	１４０	Ｇ０６Ｆ　17/60	１４０	
	19/00	３００	19/00	３００Ｎ	

審査請求　未請求　請求項の数21　ＯＬ（全９頁）　最終頁に続く

(21)出願番号　特願2000－252054(P2000－252054)

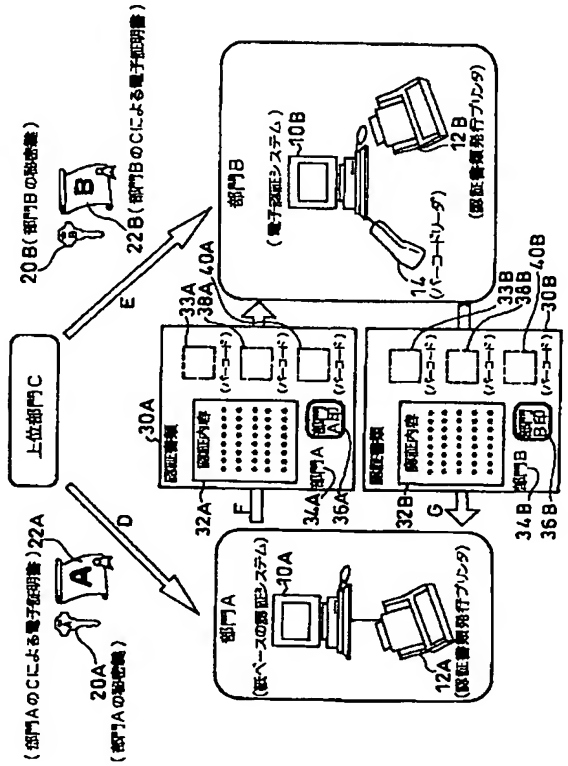
(22)出願日　平成12年８月23日(2000.8.23)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　森田　より子
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100080458
弁理士　高矢　諭　（外２名）

Ｆターム(参考)　3B041 AA10 BA15
5B035 AA15 BB01 BC00
5J104 AA09 LA03 LA06 NA02 PA13

(54)【発明の名称】　認証書類、認証用紙、及び、認証書類の発行・検証システム

(57)【要約】
【課題】　電子認証システムと紙ベースの認証システムのどちらでも利用可能な認証書類を提供する。
【解決手段】　認証書類３０Ａ、３０Ｂに、視覚により確認可能な認証内容３２Ａ、３２Ｂ、認証者情報３４Ａ、３４Ｂ及び認証者印影３６Ａ、３６Ｂと、前記認証内容３２Ａ、３２Ｂを記述した認証内容データのバーコード３３Ａ、３３Ｂ、該認証内容データを暗号化した電子署名データのバーコード３８Ａ、３８Ｂ、認証者の電子証明書データのバーコード４０Ａ、４０Ｂと共に記載する。



【特許請求の範囲】
【請求項１】視覚により確認可能な認証内容、認証者情報及び認証者印影と、
前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、
が共に記載されていることを特徴とする認証書類。
【請求項２】前記認証書類に、更に、認証機関による認証者の電子証明書データのバーコードが記載されていることを特徴とする、請求項１に記載の認証書類。
【請求項３】前記認証内容データが、マークアップ言語で記述されていることを特徴とする、請求項１又は２に記載の認証書類。
【請求項４】前記電子署名データが、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータであることを特徴とする、請求項１乃至３のいずれかに記載の認証書類。
【請求項５】前記バーコードが、２次元バーコードであることを特徴とする、請求項１乃至４のいずれかに記載の認証書類。
【請求項６】前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化されていることを特徴とする、請求項１乃至４のいずれかに記載の認証書類。
【請求項７】前記電子証明書データが、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムであることを特徴とする、請求項２に記載の認証書類。
【請求項８】認証者情報や認証者印影、及び、認証者の電子証明書データが予め印刷されていることを特徴とする認証用紙。
【請求項９】データベースから認証内容を記述した認証内容データを呼び出す手順と、
前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、
各データをバーコード化する手順と、
視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順と、
を含むことを特徴とする認証書類の発行方法。
【請求項１０】更に、認証機関による認証者の電子証明書データを呼び出す手順と、
該電子証明書データをバーコード化する手順と、
該バーコードを印刷する手順と、
を含むことを特徴とする、請求項９に記載の認証書類の発行方法。
【請求項１１】更に、前記認証内容データをマークアップ言語化する手順を含むことを特徴とする、請求項９又は１０に記載の認証書類の発行方法。
【請求項１２】更に、直接バーコード化できないデータを、テキストデータに変換する手順を含むことを特徴とする、請求項９乃至１１のいずれかに記載の認証書類の発行方法。
【請求項１３】前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成することを特徴とする、請求項９乃至１２のいずれかに記載の認証書類の発行方法。
【請求項１４】データベースから認証内容を記述した認証内容データを呼び出す手段と、
前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、
各データをバーコード化する手段と、
視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段と、
を含むことを特徴とする認証書類の発行装置。
【請求項１５】データベースから認証内容を記述した認証内容データを呼び出す手段と、
前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、
認証機関による認証者の電子証明書データを呼び出す手段と、
各データをバーコード化する手段と、
視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、
を含むことを特徴とする認証書類の発行装置。
【請求項１６】視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、
読み取った電子署名データを復号化する手順と、
該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順と、
を含むことを特徴とする認証書類の検証方法。
【請求項１７】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むことを特徴とする、請求項１６に記載の認証書類の検証方法。
【請求項１８】更に、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手順を含むことを特徴とする、請求項１６に記載の認証書類の検証方法。
【請求項１９】前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復合化するこ

【特許請求の範囲】
【請求項１】視覚により確認可能な認証内容、認証者情報及び認証者印影と、
前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、
が共に記載されていることを特徴とする認証書類。
【請求項２】前記認証書類に、更に、認証機関による認証者の電子証明書データのバーコードが記載されていることを特徴とする、請求項１に記載の認証書類。
【請求項３】前記認証内容データが、マークアップ言語で記述されていることを特徴とする、請求項１又は２に記載の認証書類。
【請求項４】前記電子署名データが、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータであることを特徴とする、請求項１乃至３のいずれかに記載の認証書類。
【請求項５】前記バーコードが、２次元バーコードであることを特徴とする、請求項１乃至４のいずれかに記載の認証書類。
【請求項６】前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化されていることを特徴とする、請求項１乃至４のいずれかに記載の認証書類。
【請求項７】前記電子証明書データが、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムであることを特徴とする、請求項２に記載の認証書類。
【請求項８】認証者情報や認証者印影、及び、認証者の電子証明書データが予め印刷されていることを特徴とする認証用紙。
【請求項９】データベースから認証内容を記述した認証内容データを呼び出す手順と、
前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、
各データをバーコード化する手順と、
視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順と、
を含むことを特徴とする認証書類の発行方法。
【請求項１０】更に、認証機関による認証者の電子証明書データを呼び出す手順と、
該電子証明書データをバーコード化する手順と、
該バーコードを印刷する手順と、
を含むことを特徴とする、請求項９に記載の認証書類の発行方法。
【請求項１１】更に、前記認証内容データをマークアップ言語化する手順を含むことを特徴とする、請求項９又は１０に記載の認証書類の発行方法。
【請求項１２】更に、直接バーコード化できないデータを、テキストデータに変換する手順を含むことを特徴とする、請求項９乃至１１のいずれかに記載の認証書類の発行方法。
【請求項１３】前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成することを特徴とする、請求項９乃至１２のいずれかに記載の認証書類の発行方法。
【請求項１４】データベースから認証内容を記述した認証内容データを呼び出す手段と、
前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、
各データをバーコード化する手段と、
視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段と、
を含むことを特徴とする認証書類の発行装置。
【請求項１５】データベースから認証内容を記述した認証内容データを呼び出す手段と、
前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、
認証機関による認証者の電子証明書データを呼び出す手段と、
各データをバーコード化する手段と、
視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、
を含むことを特徴とする認証書類の発行装置。
【請求項１６】視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、
読み取った電子署名データを復号化する手順と、
該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順と、
を含むことを特徴とする認証書類の検証方法。
【請求項１７】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むことを特徴とする、請求項１６に記載の認証書類の検証方法。
【請求項１８】更に、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手順を含むことを特徴とする、請求項１６に記載の認証書類の検証方法。
【請求項１９】前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復合化するこ

の真贋の確認を行うものとして、特開２０００－１４８７４２には、印章やサインイメージの近傍に、その管理番号及び使用番号をバーコード形式で付記すると共に、印字文書の中に、文書の管理番号及び保管機関のコードをバーコード形式で付記し、認証管理システム、及び、認証管理方法の実現のため電子文書を保管する電子文章データ保管システムと、個人や法人の印章やサイン等のイメージデータを認証データとして保管する認証データ保管システムで、相互に認証データの管理番号と文章管理番号を保管及び管理することが記載されている。

【００１４】この方法によれば、印章やサインイメージの真贋の確認は容易となるが、文書の内容はバーコード化されていないので、文書内容の電子データ化に際しては、やはり前記のような問題点を生じる。

【００１５】又、特表平９－５１２１１４には、ファクシミリでの文書送信において、元文書全体を画像スキャンし、圧縮・符号化し、バーコード化して認証することが記載されている。

【００１６】しかしながら、この方法は、特殊機能を持つファクシミリ同士のやりとりでしか利用できない。又、本文書の画像スキャンしたラスタデータをそのままやりとりするため、何らかの方法でテキストデータ化しないと、本文の内容を２次利用できない等の問題点を有していた。

【００１７】本発明は、前記従来の問題点を解消するべくなされたもので、紙ベースの認証システムと電子認証システムの両者で利用可能であり、電子データ化が容易で、且つ、改竄防止性能も高い認証書類を提供することを第１の課題とする。

【００１８】本発明は、又、前記認証書類の作成に適した認証用紙を提供することを第２の課題とする。

【００１９】本発明は、又、前記認証書類の発行方法及び装置を提供することを第３の課題とする。

【００２０】本発明は、又、前記認証書類の検証方法及び装置を提供することを第４の課題とする。

【００２１】

【課題を解決するための手段】本発明は、認証書類に、視覚により確認可能な認証内容、認証者情報及び認証者印影と、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、を共に記載することにより、前記第１の課題を解決したものである。

【００２２】更に、前記認証書類に、認証機関による認証者の電子証明書データのバーコードも記載したものである。

【００２３】又、前記認証内容データを、マークアップ言語で記述したものである。

【００２４】又、前記電子署名データを、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータとしたものである。

【００２５】又、前記バーコードを、２次元バーコードとしたものである。

【００２６】又、前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化したものである。

【００２７】又、前記電子証明書データを、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムとしたものである。

【００２８】本発明は、又、認証用紙に、認証者情報や認証者印影、及び、認証者の電子証明書データを予め印刷することにより、前記第２の課題を解決したものである。

【００２９】本発明は、又、データベースから認証内容を記述した認証内容データを呼び出す手順と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、各データをバーコード化する手順と、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順とにより、認証書類を発行するようにして、前記第３の課題を解決したものである。

【００３０】更に、認証機関による認証者の電子証明書データを呼び出す手順と、該電子証明書データをバーコード化する手順と、該バーコードを印刷する手順と、を含むようにしたものである。

【００３１】更に、前記認証内容データをマークアップ言語化する手順を含むようにしたものである。

【００３２】更に、直接バーコード化できないデータを、テキストデータに変換する手順を含むようにしたものである。

【００３３】又、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成するようにしたものである。

【００３４】本発明は、又、認証書類の発行装置を、データベースから認証内容を記述した認証内容データを呼び出す手段と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、各データをバーコード化する手段と、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段を用いて構成することにより、前記第３の課題を解決したものである。

【００３５】本発明は、又、認証書類の発行装置を、データベースから認証内容を記述した認証内容データを呼び出す手段と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、認証機関による認証者の電子証明書データを呼び出す手段と、各データをバーコード化する手段と、視覚により確認可能な認証

内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、を用いて構成することにより、前記第３の課題を解決したものである。

【００３６】本発明は、又、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、読み取った電子署名データを復号化する手順と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順とにより、認証書類を検証するようにして、前記第４の課題を解決したものである。

【００３７】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むようにしたものである。

【００３８】又は、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手順を含むようにしたものである。

【００３９】又、前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復合化するようにしたものである。

【００４０】本発明は、又、認証書類の検証装置を、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、認証機関による認証者の電子証明書データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無を判定する手段を用いて構成することにより、前記第４の課題を解決したものである。

【００４１】本発明は、又、認証書類の検証装置を、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無及び認証者の本人性を判定する手段とを用いて構成することにより、前記第４の課題を解決したものである。

【００４２】

【発明の実施の形態】以下図面を参照して、本発明の実施形態を詳細に説明する。

【００４３】今、図１に示す如く、紙ベースの認証システムで運用している部門Ａと、電子認証システムで運用している部門Ｂと、部門Ａと部門Ｂを電子認証している、例えば最上位に位置するルート認証局あるいは信頼できる中間認証局である上位（管理）部門Ｃ（認証機関）を想定する。

【００４４】前記部門Ａには、例えば、認証内容のデータベースを含むパソコン１０Ａ及び認証書類発行用のプリンタ１２Ａが備えられている。この部門Ａには、矢印Ｄに示す如く、上位部門Ｃから当該部門Ａの秘密鍵データ２０Ａと、当該部門Ａの公開鍵を含み、上位部門Ｃの電子署名がされている、部門Ａの電子証明書データ２２Ａと、上位部門Ｃの公開鍵を含む、部門Ｃの電子証明書データ（図示省略）が配布されているとする。

【００４５】又、前記部門Ｂには、例えば、部門Ａと同様のパソコン１０Ｂ及びプリンタ１２Ｂと、バーコードリーダ１４とが備えられている。この部門Ｂには、矢印Ｅに示す如く、上位部門Ｃから、当該部門Ｂの秘密鍵データ２０Ｂと、当該部門Ｂの公開鍵を含み、上位部門Ｃの電子署名がされている、部門Ｂの電子証明書データ２２Ｂと、上位部門Ｃの公開鍵を含む、部門Ｃの電子証明書データ（図示省略）を配布されているとする。

【００４６】まず、矢印Ｆに示す如く、紙ベースの認証システムの部門Ａで発行した認証書類３０Ａを、電子認証システムの部門Ｂで事務処理する場合について説明する。

【００４７】部門Ａで認証書類３０Ａを発行する手順を図２に示す。

【００４８】部門Ａでは、認証書類の発行要求者の要望に応じて、ステップ１００で認証内容３２Ａをデータベースから呼び出し、呼び出したデータを、必要に応じてＸＭＬ等のマークアップ言語で記述すると共に、バーコードの仕様上、直接バーコード化できないバイナリデータは、例えばＢａｓｅ６４でテキストデータに変換して、認証内容データとする。

【００４９】次いでステップ１０２で、該認証内容データを、例えばハッシュ化してメッセージダイジェストを作成し、部門Ａの秘密鍵データ２０Ａで暗号化して電子署名データを作成する。

【００５０】次いでステップ１０４で、必要に応じて、部門Ａの上位部門Ｃによる電子証明書データ２２Ａを呼び出す。なお、部門Ａと部門Ｂが頻繁に認証書類をやり取りする際には、事前に部門Ａと部門Ｂとが、上位部門Ｃによって認証された部門Ａと部門Ｂの電子証明書データを交換しておくことによって、認証書類の電子証明書データを省略することもできる。この場合には、ステップ１０４は不要である。

【００５１】次いでステップ１０６、１０８、１１０で、前出ステップ１００、１０２、１０４で作成された

データを、それぞれ、例えば２次元バーコード化する。なお、バーコード化する順番は任意であり、特に認証書類の電子証明書データを省略した場合には、当然ステップ１１０も不要である。

【００５２】次いでステップ１１２に進み、図１に符号３０Ａで示す如く、従来の紙の認証書類に記載されていた認証内容（ここでは文章）３２Ａ、部門Ａの名称３４Ａ、部門Ａの印影３６Ａに加えて、認証内容３２Ａのバーコード３３Ａ、ステップ１０２で作成された電子署名データのバーコード３８Ａ、及び、ステップ１０４で作成された電子証明書データのバーコード４０Ａを印刷して、紙の認証書類３０Ａとする。

【００５３】次に、前記のようにして作成された紙の認証書類３０Ａは、図３に示すような手順に従って、部門Ｂにより検証される。

【００５４】即ち、部門Ｂでは、まずステップ２００、２０２、２０４で、紙の認証書類３０Ａから、例えばバーコードリーダ１４（スキャナでも良い）を用いて、バーコード３３Ａ（認証内容）、バーコード３８Ａ（電子署名データ）、バーコード４０Ａ（電子証明書）を読み取る。この際、Ｂａｓｅ６４でテキストデータに変換されていたバイナリデータは、Ｂａｓｅ６４で逆変換してバイナリデータに戻す。又、電子証明書データのバーコードが省略されている場合には、ステップ２０４で、事前に入手している電子証明書データを呼び出す。

【００５５】次いでステップ２０６で、部門Ｃの電子証明書データを基に、例えばバーコード４０Ａに記述された部門Ａの電子証明書データ２２Ａが上位部門Ｃで認証されていることを確認したら、該電子証明書データ２２Ａに含まれる部門Ａの公開鍵データを取り出す。

【００５６】次いでステップ２０８に進み、ステップ２０６で取り出した公開鍵を用いて、ステップ２０２で読み取った電子署名データを復号化し、メッセージダイジェストｉを作成する。

【００５７】次いでステップ２１０に進み、ステップ２００で読み取った認証内容データをハッシュ化して、メッセージダイジェストiiを作成する。

【００５８】次いでステップ２１２に進み、メッセージダイジェストｉとiiを比較し、一致する場合には、ステップ２１４で、認証内容の本人認証と非改ざんを確認する。

【００５９】一方、メッセージダイジェストｉとiiが不一致の場合には、ステップ２１６に進み、認証内容の本人認証及び非改ざんを承認しない。

【００６０】このようにして、認証書類の内容の電子化、認証内容の非改ざんの証明、及び認証書類の部門Ａの本人証明を実現することができ、内容を確認した後、直ちに電子データを電子認証システムで扱うことが可能となる。

【００６１】一方、電子認証システムの部門Ｂで認証した書類を、図１の矢印Ｇに示す如く、紙ベースの認証の部門Ａで事務処理する場合には、部門Ａの場合と同様に、部門Ｂでも、従来の認証内容３２Ｂ、部門Ｂの名称３４Ｂ、部門Ｂの印影３６Ｂに加えて、認証内容をマークアップ言語で記述した認証内容データ、これをハッシュ化して部門Ｂの秘密鍵で暗号化した電子署名データ、上位部門Ｃによって証明されている部門Ｂの電子証明書データを、それぞれ例えば２次元バーコード３３Ｂ、３８Ｂ、４０Ｂ化し、紙の認証書類３０Ｂとして印刷する。この際、バイナリデータであって、バーコードの仕様上、直接バーコード化できない場合には、例えばＢａｓｅ６４でテキストデータに変換してからバーコード化する。

【００６２】この認証書類３０Ｂを、部門Ａでは、紙ベースであるので、従来と同様に、認証内容３２Ｂ、部門名称３４Ｂ、部門印３６Ｂにより目視で内容を確認する。なお、何らかの不具合等で、部門Ａから部門Ｂに認証書類を返送する必要がある場合には、部門Ｂでは、バーコードリーダ１４でバーコードを読み取って、再度内容を取り込むことが可能である。

【００６３】本実施形態においては、バーコードとして、２次元バーコードを用いているので、少ない面積で、多くの情報を記述できる。なお、バーコードの種類は、これに限定されない。

【００６４】又、本実施形態においては、バーコードの仕様上、直接バーコード化できない場合には、Ｂａｓｅ６４でテキストデータに変換してからバーコード化するようにしているので、バイナリデータであっても、バーコード化可能である。なお、バイナリデータをテキストデータに変換する方式はＢａｓｅ６４に限定されず、例えばＵＮＩＸ（登録商標）標準のｕｕｅｎｃｏｄｅや、Ｍａｃｉｎｔｏｓｈで用いられているＢｉｎＨｅｘといった方式を用いることも可能である。

【００６５】更に、本実施形態においては、マークアップ言語ＸＭＬのデータにしてからバーコード化しているので、項目と内容が明瞭となり、認証内容の２次利用が容易である。なお、マークアップ言語の種類はＸＭＬに限定されず、ＨＴＭＬ、ＴＥＸ、ＳＧＭＬ等を用いることも可能である。又、マークアップ言語化を省略することも可能である。

【００６６】なお、前記実施形態においては、全ての情報をプリンタで印刷するようにしていたが、例えば図４に示す如く、認証者情報３４や認証者印影３６、及び、認証者の電子証明書データのバーコード４０等の固定されたデータが予め印刷されている認証用紙５０を用いて、印刷の負荷を軽減することも可能である。

【００６７】本発明の適用対象は、地方自治体における証明書発行や登録処理に限定されず、一般の領収書発行や、会計処理等にも同様に用いることができることは明らかである。

【0068】

【発明の効果】本発明によれば、認証書類の内容の電子化、認証書類の非改ざんの証明、認証書類の認証者の本人証明を実現でき、紙ベースの認証システムと電子認証システムのどちらでも利用可能であるという優れた効果を有する。

【図面の簡単な説明】

【図1】本発明に係る認証書類の発行方法及び検証方法を実施するシステムの例の全体構成を示すブロック線図

【図2】本発明の実施形態における認証書類の発行手順を示す流れ図

【図3】同じく認証書類の検証手順を示す流れ図

【図4】同じく認証用紙の例を示す正面図

【符号の説明】

A、B…部門

C…上位部門（認証機関）

10A、10B…パソコン

12A、12B…プリンタ

14…バーコードリーダ

20A、20B…秘密鍵データ

22A、22B…電子証明書データ

30A、30B…認証書類

32A、32B…認証内容

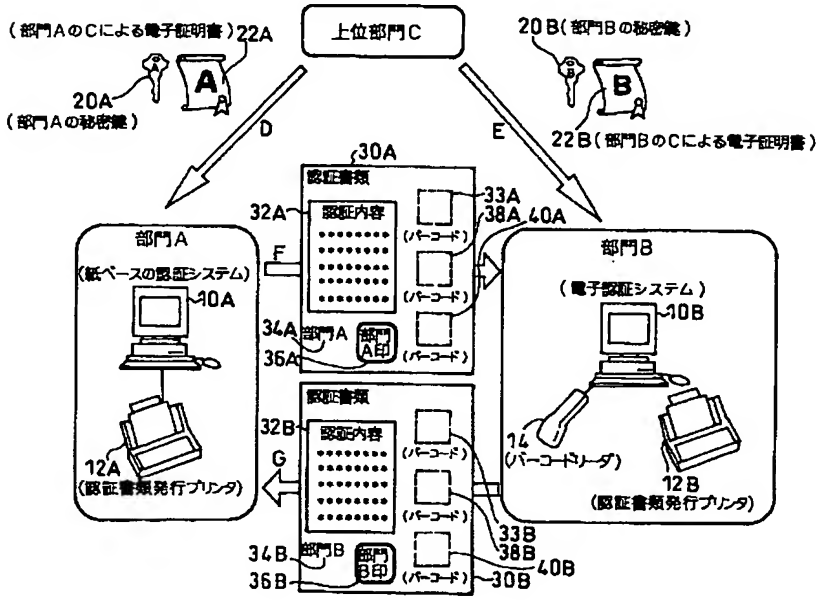
34、34A、34B…部門名称

36、36A、36B…部門印

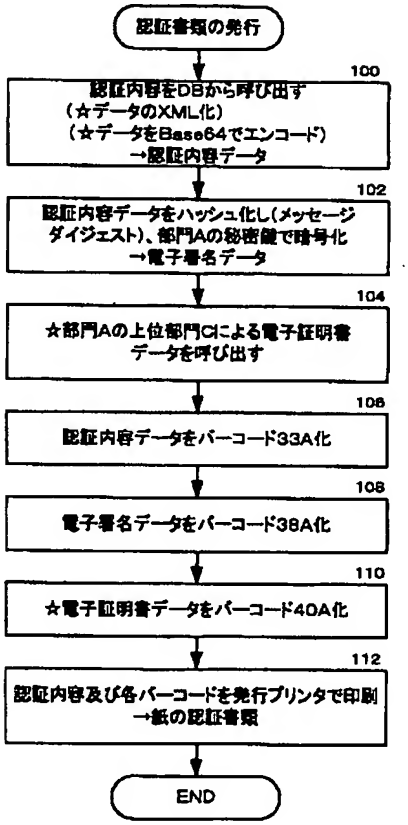
33A、33B、38A、38B、40、40A、40B…バーコード

50…認証用紙

【図1】

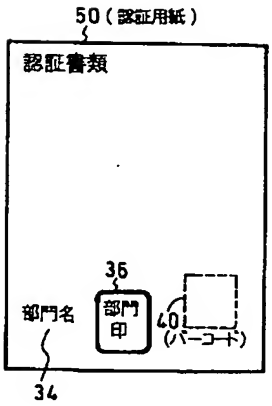


【図2】

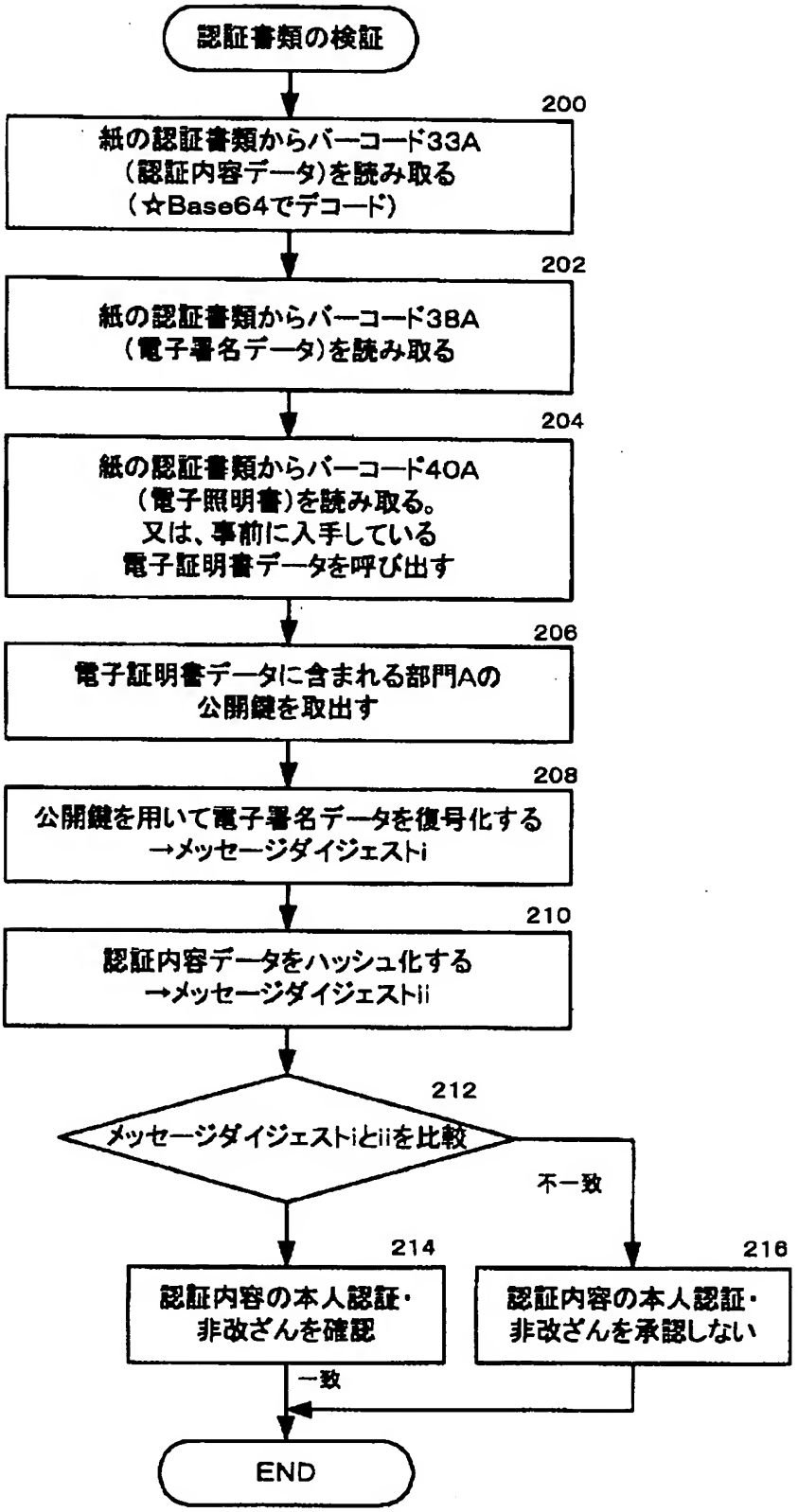


☆はオプション

【図4】



【図3】


認証書類の検証
200
紙の認証書類からバーコード33A
(認証内容データ)を読み取る
(☆Base64でデコード)
202
紙の認証書類からバーコード38A
(電子署名データ)を読み取る
204
紙の認証書類からバーコード40A
(電子照明書)を読み取る。
又は、事前に入手している
電子証明書データを呼び出す
206
電子証明書データに含まれる部門Aの
公開鍵を取出す
208
公開鍵を用いて電子署名データを復号化する
→メッセージダイジェストi
210
認証内容データをハッシュ化する
→メッセージダイジェストii
212
メッセージダイジェストiとiiを比較
不一致
214
認証内容の本人認証・
非改ざんを確認
216
認証内容の本人認証・
非改ざんを承認しない
一致
END

☆はオプション

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
G06K 19/06		G07D 7/20	
G07D 7/20		G06K 19/00	A